Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): RSW920010223-US1

I hereby certify that this correspondence is being transmitted electronically to the U.S. Patent and Trademark Office

on May 25, 2007

Signature: /Amelia Tauchen/

Typed or printed name: Amelia Tauchen

Application Number	Filed
10/007,581	12/05/2001

First Named Inventor: Brabson

Art Unit	Examiner
2135	Joseph T. Pan

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [X] attorney or agent of record. Registration number 38,904
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/David C. Hall/
Signature

David C. Hall
Typed or printed name

919-854-1400
Telephone number

May 25, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

[X] *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Attorney's Docket No.: RSW920010223-US1/5577-352 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Brabson et al.
Serial No.: 10/007,581
Filed: December 5, 2001
For: **OFFLOAD PROCESSING FOR SECURITY SESSION ESTABLISHMENT AND CONTROL**

Confirmation No.: 3407
Group Art Unit: 2135
Examiner: Joseph T. Pan

Date: May 25, 2007

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted electronically to the U.S. Patent and Trademark Office on May 25, 2007.

Amelia Tauchen

REASONS IN SUPPORT OF APPLICANTS' PRE-APPEAL BRIEF REQUEST FOR REVIEW

This document is submitted in support of the Pre-Appeal Brief Request for Review that is filed concurrently herewith along with a Notice of Appeal in compliance with 37 C.F.R. 41.31 and with the rules set out in the OG Notice of July 12, 2005 for the New Appeal Brief Conference Pilot Program.

It is not believed that an extension of time and/or additional fee(s)-including fees for net addition of claims-are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. §1.136(a). Any additional fees believed to be due in connection with this paper may be charged to our Deposit Account 09-0461.

REMARKS

Applicants hereby request a Pre-Appeal Brief Review (hereinafter "Request") of the claims finally rejected in the Final Office Action mailed February 28, 2007 ("Final Office

Action") and the Advisory Action mailed May 1, 2007 ("Advisory Action"). The Request is provided herewith in accordance with the rules set out in the OG Notice of July 12, 2005.

Applicants submit that the rejections are based on clear errors, and that the Final Office Action and Advisory Opinion have failed to establish a prima facie case of obviousness with respect to the rejected claims. Accordingly, Applicants request review of the present application by an appeal conference prior to the filing of an appeal brief. In the interest of brevity and without waiving the right to argue additional grounds should this Petition be denied, Applicants will only discuss some particular errors made in the rejections of the Independent Claims.

Independent Claims 1 and 33-35 stand rejected as unpatentable over U.S. Patent No. 6,141,705 to Anand et al. ("Anand") in view of U.S. Patent Publication No. 2003/0014623 to Freed et al. ("Freed").

Claim 1 recites as follows:

> 1. A method of performing security processing in a computing network comprising a local unit having an operating system kernel executing at least one application program, comprising:
>
> receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit;
>
> providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the remote unit; and
>
> providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component.

The Final Office Action asserted that Anand teaches receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit, providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the remote unit, and providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component. Final Office Action , pp. 2-3. In support of this assertion, the Final Office Action cited the passage of Anand at col. 10, lines 27-47 (Final Office Action, pages 2-3).

The Final Office Action cited Anand col. 3, lines 9-23 (Final Office Action, page 9), and both the Advisory Action and the Final Office Action cited Anand col. 3, lines 39-44 (Final Office Action, page 3; Advisory Action, Continuation Sheet). While the cited passages of Anand may indicate that certain security functions may be performed at NIC hardware, the Final Office Action and the Advisory Action mistakenly interpret the cited passages of Anand as teaching providing a request from an operating system *kernel* to a security offload component directing the security offload component to secure a communication with a remote unit.

Rather, as explained in Applicants' Request For Reconsideration filed April 20, 2007, Anand expressly teaches that requests for security offload processing are issued by transport protocol drivers, which are not part of an operating system kernel. See Request For Reconsideration, pages 10-12. Accordingly, Anand fails to teach at least the recitations of Claim 1 of receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit, providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the remote unit, and providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component.

Furthermore, the Final Office Action and the Advisory Action erroneously assert that Anand discloses that the transport protocol driver is implemented in the operating system kernel. Final Office Action at 10. In support, the Final Office Action cited the following passage of Anand:

> In a preferred embodiment of the present invention, in the Windows NT layered networking architecture, a transport protocol driver, or transport, is implemented with an appropriate program method so as to be capable of querying each of the device driver(s) associated with the corresponding NIC(s) connected to the computer.

Anand, col. 3, lines 45-50. Applicants submit that the cited passage describes the "Windows NT layered networking architecture," not the Windows NT operating system. Moreover, the passage

states that the transport protocol driver "is implemented with an appropriate program method," and does not indicate that the driver is somehow implemented in the operating system kernel.

The Advisory Action asserts that, as used in the above-cited passage, the term "Windows NT environment" refers to the Windows NT operating system. See Advisory Action, Continuation Sheet. Applicants submit that interpretation of Anand expressed in the Final Office Action and the Advisory Action clearly ignores the term "environment," which is understood by a skilled person not to refer to the operating system itself, but to the environment created by the operating system in which application programs operate. That is, in the context of computer systems, the term "environment" refers not to the operating system kernel, but to a computer interface from which various tasks can be performed. See Merriam-Webster Online Dictionary, definition of "environment" (http://www.m-w.com/dictionary/environment)(" 4 : a computer interface from which various tasks can be performed <a programming environment>").

Attention is directed to Microsoft Knowledge Base Article 100843, available at http://support.microsoft.com/kb/100843. This article relates to the setting of environment variables in Windows NT, and states "All environment variables and the paths set in the AUTOEXEC.BAT file are used to create the *Windows NT environment*." (emphasis added). Clearly, the Knowledge Base article, written by the manufacturer of the Windows NT operating system, is not stating that an AUTOEXEC.BAT file is creating a Windows NT operating system *kernel*, as the erroneous interpretation in the Final Office Action and the Advisory Action would purport. The term "Windows NT environment" is used consistently with the dictionary definition in numerous other Knowledge Base articles.

Furthermore, the cited passage of Anand is consistent with this interpretation of the term "Windows NT environment," as the cited passage discusses implementation of drivers that perform various tasks on a computer. Accordingly, a skilled person would not understand the term "Windows NT environment" used in the cited passage of Anand to refer to the Windows NT operating system kernel, but rather would understand the term to refer to a Windows NT computer interface from which various tasks can be performed.

This understanding of the term "Windows NT environment" is consistent with Applicants' understanding of the teaching of Anand, namely, that in Anand a transport protocol driver, as opposed to the operating system kernel, can issue requests for security offload processing. Anand's teaching therefore contrasts sharply with the recitations of Claim 1 that provide "receiving a first request at the operating system kernel from the application program to initiate a communication with a remote unit, providing a second request from the operating system kernel to a security offload component which performs security handshake processing, the second request directing the security offload component to secure the communication with the remote unit, and providing a control function in the operating system kernel for initiating operation of the security handshake processing by the security offload component" (emphasis added). Moreover, Anand does not suggest the benefits of controlling the operation of a security offload component using a control function in an operating system kernel rather than requiring such control functionality to be implemented in an application program.

Accordingly, Applicants submit that, properly understood, Anand does not teach or suggest many of the recitations of Independent Claim 1. Independent Claims 33-35 are patentable for similar reasons based on corresponding recitations thereof.

For at least these reasons, Applicants submit that the Final Office Action and Advisory Opinion have relied on a clearly erroneous understanding of Anand in formulating the rejections set forth therein, and have failed to establish that the combination of Anand and Freed discloses each and every recitation of Independent Claims 1 and 33-35.

Respectfully submitted,

David C. Hall
Registration No. 38,904

Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)